

## INFORMATION DISCLOSURE CITATION

(Use several sheets if necessary)

Atty. Docket No.  
35.C11664 DIDivision of Appln  
No. 08/706,491Applicant  
KEIICHI IWAMURAFiling Date  
Concurrently HerewithGroup 2164  
Unknown

## U.S. PATENT DOCUMENTS

*Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date If Appropriate
DOF	5 6 6 6 4 1 9	09/1997	Yamamoto et al.	308	28	11-29-1994
DOF	5 6 5 0 6 0 4	07/1997	Marcous et al.	235	379	2-22-1995
DOF	5 6 3 4 0 1 2	05/1997	Stefik et al.	395	239	11-23-1994
DOF	5 6 0 0 7 2 0	02/1997	Iwamura et al.	380	1	7-19-1994
DOF	4 3 7 0 6 4 9	01/1983	Fuerle	340	825.35	5-19-1981

## FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation Yes No
DOF	4 - 6 4 1 2 9	02/1992	Japan			Abstract
DOF	2 - 4 4 4 4 7	02/1990	Japan			Abstract
	64 - 6 8 8 3 5	03/1989	Japan			Abstract
DOF	60 1 9 1 3 2 2	09/1985	Japan			Abstract
DOF	60 - 7 7 2 1 8	05/1985	Japan			Abstract

## OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Page, Etc.)

DOF		T. Okamoto and A. Shiraishi, "A fast signature scheme based on quadratic inequalities", IEEE Symp. on Security and Privacy, pp 123-132, April 22-24, 1985
DOF		H. Ong, C.P. Schnorr and A. Shamir, "An efficient signature scheme based on quadratic equations", ACM Symp. on Theory of Computing, 4/30-5/2/84, pp 208-216.
DOF		S. Goldwasser, S. Micali and A. Yao, "Strong signature schemes", ACM Symp. on Theory of Computing, 4/25/-27/83, pp 431-439.

EXAMINER

DATE CONSIDERED

Daniel A. Felten

2-20-2001

\*Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Form PTO-FB-A820  
(also form PTO-1449)  
(June 16, 1999)

Patent and Trademark Office-U.S. DEPARTMENT of COMMERCE

Page 1 of 3

## INFORMATION DISCLOSURE CITATION

(Use several sheets if necessary)

Atty. Docket No.  
35.C11664 DI

Division of Appln  
No. 08/706,491

Applicant

KEIICHI IWAMURA

Filing Date

Concurrently Herewith

| Group

~~Unknown~~ 2164

## U.S. PATENT DOCUMENTS

*Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date If Appropriate
DA	5103392	04/1992	Mori	395	925	12-5-1990

## FOREIGN PATENT DOCUMENTS

[illegible]

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Page, Etc.)

204			T. Matsumoto and H. Imai, "A class of asymmetric cryptosystems based on polynomials over finite rings", IEEE International Symp. on Information Theory, 1983, 9/83, Abstract pp 131-132.
209			H.C. Williams, "A modification of the RSA public-key encryption procedure", IEEE Trans. of Inf. Theory, 11/80, pp. 726-729.
209			A. Shamir and R.E. Zippel, "On the security of the Merkle3-Hellman cryptographic scheme", IEEE trans. on Inf. Theory, 5/80, pp 339-340.

**EXAMINER**

DATE CONSIDERED

David A. Feltner

2-20-2001

\***Examiner:** Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Form PTO-FB-A820  
(also form PTO-1449)  
(June 16, 1999)

Patent and Trademark Office-U.S. DEPARTMENT of COMMERCE

Page 2 of 3

## INFORMATION DISCLOSURE CITATION

(Use several sheets if necessary)

Atty. Docket No.

35.C11664 DI

Division of Appln

No. 08/706,491

Applicant

KEIICHI IWAMURA

Filing Date

Concurrently Herewith

Group

Unknown

## U.S. PATENT DOCUMENTS

*Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date If Appropriate

## FOREIGN PATENT DOCUMENTS

	Document Number	Date	Country	Class	Subclass	Translation	
						Yes	No

## OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Page, Etc.)

1978		M. Rabin, "Digitalized signatures and public-key cryptosystems, MIT/LCS/TR-212, Technical Report MIT. Jan. 1979, pp 1-16.
1978		R.C. Merkle and M.E. Hellman, "Hiding Information and signatures in trapdoor knapsacks", IEEE Trans. on Inf. Theory, 9/78, pp 525-530.
1978		A. Shamir, "A fast signature scheme", report MIT/LCS/TM-107, MIT Laboratory for computer science, July 1978, pp 1-17.
1978		R.L. Rivest, A. Shamir and I. Adleman, "A method of obtaining digital signatures and public key cryptosystems, Comm. of ACM, 1978, pp 120-126.
1978		R.J. McEliece, "A public-key cryptosystem based on algebraic coding theory", DSN Progress Rep. Jet Propulsion Lab. Jan.-Feb. 1978, pp 114-116.

EXAMINER

DATE CONSIDERED

Daniel S. Felker

02-20-2001

\*Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Form PTO-FB-A820

(also form PTO-1449)

(June 16, 1999)

Patent and Trademark Office-U.S. DEPARTMENT of COMMERCE

Page 3 of 3